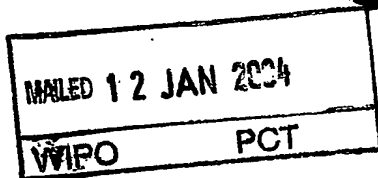


03 OCT. 2003



Rec'd PCT/PTO 31 MAR 2005

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 09 SEP. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ
PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 260899

<p>REMISE DES PIÈCES DATE 04 OCT 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0212325 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 04 OCT. 2002</p>		<p>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE BREVALEX 3, rue du Docteur Lancéreaux 75008 PARIS</p>	
<p>Vos références pour ce dossier (facultatif) SP 21975 DB I2002.021</p>			
<p>Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie</p>			
<p>2 NATURE DE LA DEMANDE</p>		<p>Cochez l'une des 4 cases suivantes</p>	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<p><i>Demande de brevet initiale</i> N° _____ Date ____/____/____</p> <p><i>ou demande de certificat d'utilité initiale</i> N° _____ Date ____/____/____</p>			
<p>Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i></p>		<p><input type="checkbox"/> N° _____ Date ____/____/____</p>	
<p>3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)</p> <p>LOGICIEL EMBARQUE ET PROCEDE D'AUTHENTIFICATION DE CELUI-CI</p>			
<p>4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE</p>		<p>Pays ou organisation _____ N° _____ Date ____/____/____ Pays ou organisation _____ N° _____ Date ____/____/____ Pays ou organisation _____ N° _____ Date ____/____/____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»</p>	
<p>5 DEMANDEUR</p>		<p><input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»</p>	
Nom ou dénomination sociale		CANAL + TECHNOLOGIES	
Prénoms			
Forme juridique		Société anonyme	
N° SIREN			
Code APE-NAF			
Adresse	Rue	34, place Raoul Dautry	
	Code postal et ville	75015	PARIS
Pays		FRANCE	
Nationalité		Française	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			

REMISE DES PIÈCES DATE 4 OCT 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0212325 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI		DB 540 W / 260899	
Vos références pour ce dossier : <i>(facultatif)</i>		SP 21975 DB I2002.021			
6 MANDATAIRE					
Nom		DU BOISBAUDRY			
Prénom		Dominique			
Cabinet ou Société		BREVALEX			
N° de pouvoir permanent et/ou de lien contractuel					
Adresse	Rue	3, rue du Docteur Lancereaux			
	Code postal et ville	75008	PARIS		
N° de téléphone <i>(facultatif)</i>		01 53 83 94 00			
N° de télécopie <i>(facultatif)</i>		01 45 63 83 33			
Adresse électronique <i>(facultatif)</i>		brevets.patents@brevaalex.com			
7 INVENTEUR (S)					
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée			
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)			
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>			
Paiement échelonné de la redevance		Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input type="checkbox"/> Non			
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):			
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes					
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)		VISA DE LA PRÉFECTURE OU DE L'INPI M. BLANCANEAU			

LOGICIEL EMBARQUE ET PROCEDE D'AUTHENTIFICATION DE CELUI-CI

DESCRIPTION

5 **DOMAINE TECHNIQUE**

L'invention concerne un logiciel embarqué et un procédé d'authentification de celui-ci, notamment dans le domaine des décodeurs en télévision numérique.

10 **ETAT DE LA TECHNIQUE ANTERIEURE**

Dans les dispositifs de l'art connu, un test d'intégrité d'un logiciel embarqué est généralement réalisé en calculant, à l'aide d'un outil externe, une signature de référence de ce logiciel
15 représentative de celui-ci et en insérant celle-ci dans ce logiciel. Pendant la phase d'initialisation du logiciel, celui-ci calcule sa propre signature et compare cette signature avec la signature de référence. Si ces signatures sont différentes, le logiciel exécute
20 un logiciel spécifique à une procédure de défense sinon il continue normalement.

Dans le cas d'une authentification d'un tel logiciel, on souhaite s'assurer de la provenance de celui-ci. Une solution connue consiste à reprendre le
25 principe du test d'intégrité et à le combiner avec un algorithme cryptographique asymétrique : la signature de référence est chiffrée avec une clé privée et le résultat est intégré, sous forme d'un certificat, au logiciel. Pendant la phase de contrôle, la signature de
30 référence est déchiffrée avec une clé publique intégrée

au logiciel avant d'être comparée à la signature de référence.

Un premier document de l'art connu, la norme ETSI TS 101 812 V1-1-1 intitulée "Digital Video
5 Broadcasting (DVB) Multimédia Home Platform (MHP) Spécification 1.0" (2000-07) notamment les sections 12.2 et 12.7, décrit la mise en œuvre d'une authentification de logiciel téléchargé dans un terminal en réalisant une authentification par certificat dudit logiciel
10 téléchargé au moyen d'un logiciel embarqué dans ledit terminal.

Un second document de l'art connu, US 6,167,521, décrit un procédé de téléchargement d'un nouveau logiciel dans un système, qui a pour objet
15 d'éviter que ce nouveau logiciel téléchargé ne s'attaque à un logiciel déjà installé dans ce système, ou réciproquement d'éviter que le logiciel déjà installé ne s'attaque au nouveau logiciel, notamment lorsque les propriétaires de ces deux logiciels n'ont
20 pas confiance l'un en l'autre.

Plus précisément pour réaliser une authentification de logiciel, il est connu, comme illustré sur la figure 1, d'utiliser un logiciel contenu dans une mémoire dans une première partie 10
25 fixe, c'est-à-dire protégée en écriture, pour authentifier un logiciel applicatif d'une seconde partie 11, qui peut avoir été téléchargée, en utilisant un certificat 12 situé dans cette seconde partie 11.

Ainsi, dans le domaine du décodeur,
30 lorsqu'un client vient trouver le fournisseur de service avec un nouveau logiciel applicatif, celui-ci

lui fournit un logiciel de vérification de ce logiciel applicatif et un certificat à associer à ce dit logiciel applicatif.

5 Mais dans une telle solution, rien ne permet au fournisseur du premier logiciel de s'assurer que la procédure d'authentification a bien eu lieu.

L'invention a pour objet de permettre au fournisseur de s'assurer que cette authentification a bien eu lieu et que ses droits ont donc bien été
10 respectés par le client.

EXPOSÉ DE L'INVENTION

La présente invention propose donc un
15 procédé d'authentification d'un logiciel téléchargé dans un terminal, ledit procédé comprenant une étape d'authentification par certificat dudit logiciel téléchargé au moyen d'un logiciel embarqué dans ledit terminal, caractérisé en ce qu'il comprend, en outre,
20 une étape d'authentification par certificat, lors de l'exécution dudit logiciel téléchargé, dudit premier logiciel embarqué au moyen d'un module logiciel d'authentification associé audit logiciel téléchargé.

25 Avantageusement le premier logiciel embarqué authentifie le logiciel téléchargé au moyen d'une librairie d'authentification et d'un premier certificat ; le premier logiciel embarqué et la librairie d'authentification forment une première
30 partie de mémoire protégée en écriture, le logiciel

téléchargé et ce premier certificat forment une seconde partie de mémoire chargeable.

Avantageusement, la première partie comporte également un second certificat, la seconde
5 partie comporte en outre un logiciel de vérification, et, une fois le logiciel téléchargé authentifié, le logiciel de vérification authentifie le premier logiciel au moyen de la librairie d'authentification et du second certificat.

10 Avantageusement, ces deux authentifications successives ont lieu à l'initialisation. La seconde partie peut être téléchargée.

L'invention concerne également un logiciel embarqué comprenant une première partie de mémoire
15 protégée en écriture formée d'un premier logiciel et d'une librairie d'authentification, et une seconde partie comportant un logiciel applicatif et un premier certificat, caractérisé en ce que la première partie comprend, en outre, un second certificat, et en ce que
20 la seconde partie comporte en outre un logiciel de vérification.

Ce logiciel peut être utilisé par exemple dans un décodeur de télévision numérique, dans un terminal de type PC ("personal computer"), ou dans tout
25 autre appareil embarqué.

BREVE DESCRIPTION DES DESSINS

La figure 1 illustre un procédé d'authentification de l'art connu.

30 La figure 2 illustre le procédé d'authentification de l'invention.

La figure 3 illustre un exemple de certificat.

La figure 4 illustre un exemple de signature.

5

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

Dans le procédé de l'invention, comme dans le procédé de l'art connu illustré sur la figure 1, un premier logiciel contenu dans une première partie 10 de mémoire protégée en écriture, authentifiée, par exemple dans la phase d'initialisation, un second logiciel, qui est le logiciel applicatif, situé dans une seconde partie 11 chargeable en utilisant une librairie d'authentification située dans la première partie et un certificat 12 situé dans cette seconde partie 11.

Le terme "certificat" ayant un sens bien particulier (Une identité électronique qui est émise par une tierce partie de confiance pour une personne ou une entité réseau, Chaque certificat étant signé avec la clé privée de signature d'une autorité de certification.) et trop limitatif dans les techniques d'authentification, le terme "certificat" utilisé dans la présente description entend couvrir également, plus généralement, les termes signature, CRC ou autres données nécessaires à vérifier l'authenticité/intégrité d'un logiciel.

Dans le procédé de l'invention, la première partie 10 comporte, en outre, un second certificat 13, comme illustré sur la figure 2. La seconde partie 11 comporte, en outre, un logiciel de vérification. Ce logiciel de vérification, une fois le logiciel

applicatif authentifié, authentifie le premier logiciel au moyen de la librairie d'authentification et du second certificat.

Un tel procédé permet au fournisseur du premier logiciel de s'assurer que le client qui utilise le logiciel applicatif respecte bien ses droits.

Dans un exemple de réalisation, le format du certificat, illustré sur la figure 3 est le suivant:

◦ En-tête :

- CLP ("Certificate Location Pattern") : motif donnant la situation du certificat pour trouver le certificat d'authentification dans la mémoire (par exemple 8 octets),

- RFU ("Reserved for Future Use") : réservé pour un usage ultérieur (par exemple 1 octet),

- K : numéro de clé à utiliser (par exemple 1 octet),

◦ Signature (par exemple 128 octets) qui est le résultat d'un chiffrement RSA, avec une clé privée, de 1024 bits du message illustré sur la figure 4.

La signature de 1024 bits commence par un octet à 0 pour permettre son chiffrement RSA, le reste est rempli aléatoirement d'une manière différente avant chaque chiffrement.

A l'offset H_CODE_OFFSET par rapport au début du message, on trouve un Hash code SHA1 sur 20 octets. Ce H_CODE est précédé d'un motif CHECK_PATTERN dont le rôle est de permettre la distinction entre un mauvais déchiffrement (rang ou valeur de clé publique, algorithme, certificat incohérent) et un mauvais H_CODE lors de la vérification d'intégrité.

REVENDICATIONS

- 5 1. Procédé d'authentification d'un logiciel
téléchargé dans un terminal, ledit procédé comprenant
une étape d'authentification par certificat dudit
logiciel téléchargé au moyen d'un logiciel embarqué
dans ledit terminal, caractérisé en ce qu'il comprend,
10 en outre, une étape d'authentification par certificat,
lors de l'exécution dudit logiciel téléchargé, dudit
premier logiciel embarqué au moyen d'un module logiciel
d'authentification associé audit logiciel téléchargé.
- 15 2. Procédé selon la revendication 1, dans
lequel le premier logiciel embarqué authentifie le
logiciel téléchargé au moyen d'une librairie
d'authentification et d'un premier certificat, dans
lequel le premier logiciel embarqué et la librairie
20 d'authentification forment une première partie de
mémoire (10) protégée en écriture, et dans lequel le
logiciel téléchargé et le premier certificat (12)
forment une seconde partie de mémoire (11) chargeable.
- 25 3 Procédé selon la revendication 2, dans
lequel la première partie (10) comporte également un
second certificat (13), dans lequel la seconde partie
(11) comporte en outre un logiciel de vérification, et
dans lequel, une fois le logiciel téléchargé
30 authentifié, le logiciel de vérification authentifie le

REVENDICATIONS

5 1. Procédé d'authentification d'un logiciel
téléchargé dans un terminal, ledit procédé comprenant
une étape d'authentification par certificat dudit
logiciel téléchargé au moyen d'un logiciel embarqué
dans ledit terminal, caractérisé en ce qu'il comprend,
10 en outre, une étape d'authentification par certificat,
lors de l'exécution dudit logiciel téléchargé, dudit
premier logiciel embarqué au moyen d'un module logiciel
d'authentification associé audit logiciel téléchargé.

15 2. Procédé selon la revendication 1, dans
lequel le premier logiciel embarqué authentifie le
logiciel téléchargé au moyen d'une librairie
d'authentification et d'un premier certificat, dans
lequel le premier logiciel embarqué et la librairie
20 d'authentification forment une première partie de
mémoire (10) protégée en écriture, et dans lequel le
logiciel téléchargé et le premier certificat (12)
forment une seconde partie de mémoire (11) chargeable.

25 3 Procédé selon la revendication 2, dans
lequel la première partie (10) comporte également un
second certificat (13), dans lequel la seconde partie
(11) comporte en outre un logiciel de vérification, et
dans lequel, une fois le logiciel téléchargé
30 authentifié, le logiciel de vérification authentifie le

premier logiciel embarqué au moyen de la librairie d'authentification et du second certificat (13).

4. Procédé selon la revendication 1, dans lequel ces deux authentifications successives ont lieu à l'initialisation.

5. Procédé selon la revendication 2, dans lequel la seconde partie (11) est téléchargée.

10

6. Logiciel embarqué comprenant une première partie de mémoire (10) protégée en écriture formée d'un premier logiciel et d'une librairie d'authentification, et une seconde partie de mémoire (11) comportant un logiciel applicatif et un premier certificat (12), caractérisé en ce que la première partie comprend, en outre, un second certificat (13), et en ce que la seconde partie comporte, en outre, un logiciel de vérification.

20

premier logiciel embarqué au moyen de la librairie d'authentification et du second certificat (13).

4. Procédé selon la revendication 1, dans
5 lequel ces deux authentifications successives ont lieu à l'initialisation.

5. Procédé selon la revendication 2, dans
10 lequel la seconde partie (11) est téléchargée.

6. Logiciel embarqué comprenant une
première partie de mémoire (10) protégée en écriture
comportant un premier logiciel, une librairie
d'authentification, et un second certificat (13), et
15 une seconde partie de mémoire (11) comportant un
logiciel applicatif, un premier certificat (12), et un
logiciel de vérification, pour l'exécution des étapes
du procédé selon l'une quelconque des revendications 1
à 5, lorsque ledit logiciel est exécuté sur un
20 ordinateur.

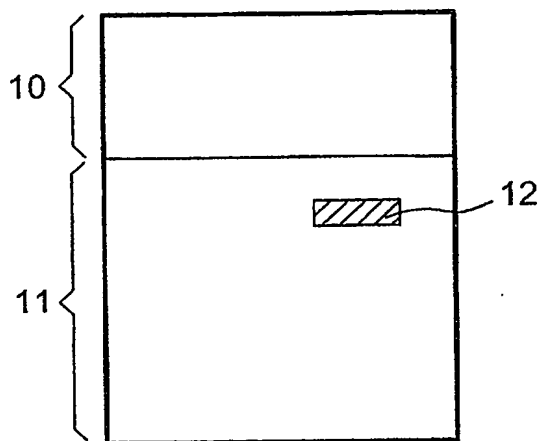


FIG. 1

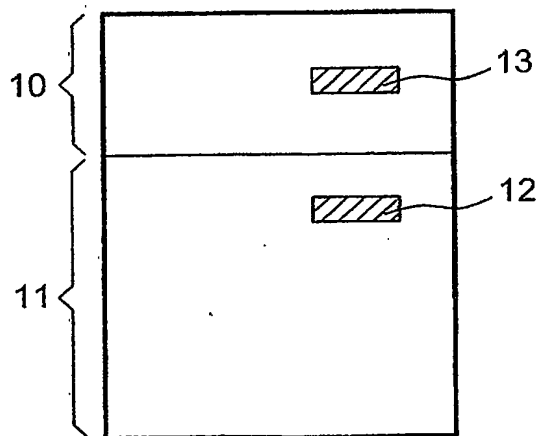


FIG. 2

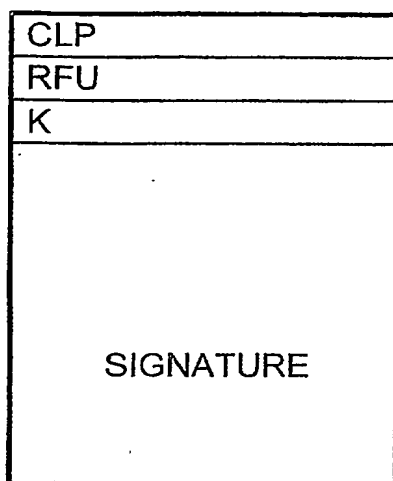


FIG. 3

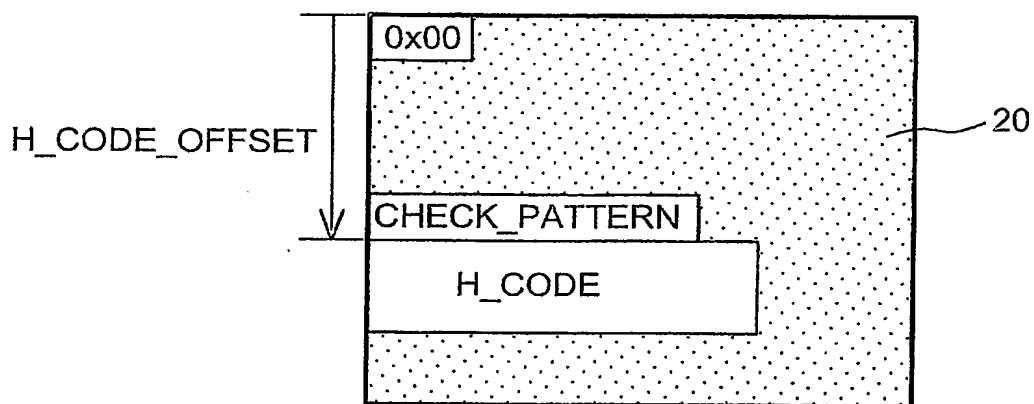


FIG. 4

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 27060

Vos références pour ce dossier (facultatif)	SP 21975/DB
N° D'ENREGISTREMENT NATIONAL	02.12325 du 04.10.2002

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

LOGICIEL EMBARQUE ET PROCEDE D'AUTHENTIFICATION DE CELUI-CI.

LE(S) DEMANDEUR(S) :

CANAL+ TECHNOLOGIES
34, Place Raoul Dautry
75015 PARIS

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1	Nom	CHAU
	Prénoms	Hervé
Adresse	Rue	31 avenue Ampère
	Code postal et ville	75014 20 CHAMPS SUR MARNE
Société d'appartenance (facultatif)		
2	Nom	SARFATI
	Prénoms	Jean-Claude
Adresse	Rue	2-4 Place d'Oberusel
	Code postal et ville	93180 10 EPINAY S/ SEINE
Société d'appartenance (facultatif)		
3	Nom	
	Prénoms	
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)

DU (DES) DEMANDEUR(S)

OU DU MANDATAIRE

(Nom et qualité du signataire)

PARIS LE 7 Novembre 2002
D. DU BOISBAUDRY

PCT Application
FR0350073

